FITTING IDEALS FOR FINITELY PRESENTED ALGEBRAIC DYNAMICAL SYSTEMS

M. EINSIEDLER AND T. WARD

Abstract. We consider a class of algebraic dynamical systems introduced by Kitchens and Schmidt. Under a weak finiteness condition – the Descending Chain Condition – the dual modules have finite presentations. Using methods from commutative algebra we show how the dynamical properties of the system may be deduced from the Fitting ideals of a finite free resolution of the finitely presented module. The entropy and expansiveness are shown to depend only on the first Fitting ideal (and certain multiplicity data) which gives an easy computation: in particular, no syzygy modules need to be computed.

For "square" presentations (in which the number of generators is equal to the number of relations) all the dynamics is visible in the first Fitting ideal and certain multiplicity data, and we show how the dynamical properties and periodic point behaviour may be deduced from the determinant of the matrix of relations.

1. Introduction

A natural family of measure–preserving $\mathbb{Z}^d$–actions are provided by commuting automorphisms of compact abelian groups. Such actions are amenable to analysis using methods from commutative algebra and commutative harmonic analysis. The resulting theory, described in the papers [4], [6], [8], [10], [12], and the monograph [11] associates to such a dynamical system a module over the ring of Laurent polynomials in d variables with integer coefficients, and then relates various dynamical properties of the action to algebraic or geometric properties of the corresponding module. This singles out for attention the class of systems corresponding to Neotherian modules (the systems satisfying the *Descending Chain Condition* of Kitchens and Schmidt, [4]) and raises the problem of computing the set of associated primes of such modules.

Our purpose here is to exploit standard methods from commutative algebra to study the dynamical systems corresponding to Noetherian modules described via a *finite presentation*. Before describing this we recall the algebraic description of such actions in [4]. Let $R = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ be the ring of Laurent polynomials with integral coefficients in the commuting variables $u_1, \dots, u_d$. If α is a $\mathbb{Z}^d$–action by automorphisms of the compact, abelian group X, then the dual (character) group $M = \hat{X}$ of X is an R-module under the dual R–action

$$f \cdot a = \sum_{\mathbf{m} \in \mathbb{Z}^d} c_f(\mathbf{m}) \beta_{\mathbf{m}}(a)$$

Date: July 20 1998.

1991 *Mathematics Subject Classification.* 22D40, 58F20.

The first author gratefully acknowledges support from a London Mathematical Society Scheme 4 grant and the hospitality of the University of East Anglia where this work was done.

for all $a \in M$ and $f = \sum_{\mathbf{m}\in\mathbb{Z}^d} c_f(\mathbf{m})u^{\mathbf{m}} \in R$, where $u^{\mathbf{n}} = u_1^{n_1}\cdots u_d^{n_d}$ for every $\mathbf{n} = (n_1,\dots,n_d) \in \mathbb{Z}^d$, and where $\beta_{\mathbf{n}} = \widehat{\alpha_{\mathbf{n}}}$ is the automorphism of $M = \hat{X}$ dual to $\alpha_{\mathbf{n}}$. In particular,

$$\widehat{\alpha_{\mathbf{n}}}(a) = \beta_{\mathbf{n}}(a) = u^{\mathbf{n}} \cdot a$$

for all $\mathbf{n} \in \mathbb{Z}^{\mathbf{d}}$ and $a \in M$. Conversely, if M is an R-module, and

$$\beta_{\mathbf{n}}^M(a) = u^{\mathbf{n}} \cdot a$$

for every $\mathbf{n} \in \mathbb{Z}^d$ and $a \in M$, then we obtain a $\mathbb{Z}^d$-action

$$\alpha^M : \mathbf{n} \to \alpha_{\mathbf{n}}^M = \widehat{\beta_{\mathbf{n}}^M}$$

on the compact, abelian group

$$X^M = \widehat{M}$$

dual to the $\mathbb{Z}^d$-action $\beta^M : \mathbf{n} \to \beta_{\mathbf{n}}^M$ on M.

The dynamical system α^M on X_M satisfies the Descending Chain Condition (any decreasing sequence of closed α^M–invariant subgroups of X_M stabilizes) if and only if the R–module is Noetherian by Theorem 11.4 in [4]. We assume from now on that M is a Noetherian module, in which case it has a finite presentation of the form

$$M = M_A \cong R^k/AR^n, \tag{1}$$

where M_A is generated as an R–module by a subset with k elements and the $k \times n$ matrix A defines the various relations in M_A. Since free modules are not very interesting, we assume that the rank of A is k. If this is not the case, then M_A has a free submodule L with the property that M_A/L has a finite presentation in the form (1) with $\mathrm{rank}(A) = k$.

In accordance with the spirit of the monograph [11], we would like then to be able to describe the dynamical properties of the $\mathbb{Z}^d$–action α^{M_A} in terms of the matrix A. Roughly speaking, we are able to (describe how to) compute all the associated primes of M_A from A using Auslander–Buchsbaum theory. This is enough to describe – in principle – the dynamical properties of α^{M_A}. For the special case $k = n$, or more generally, of *principal* associated primes, we are also able to find the multiplicities of the various associated primes, which allows the entropy of α^{M_A} to be computed. This means in particular that the entropy of α^{M_A} can be computed, and the expansiveness of α^{M_A} can be decided, without computing any syzygy modules.

Methods taken from commutative algebra are standard and may all be found for example in Eisenbud's book [3]. We are grateful to Prof. Rodney Sharp for pointing us to the right part of [3].

By "entropy" we mean topological entropy, as defined in Section 13 of Schmidt's monograph [11].

2. Language from commutative algebra

Let S be a commutative ring (recall that R is the ring of Laurent polynomials in d variables with integer coefficients). The basic terminology for an S–module M may be found in any commutative algebra book. A prime ideal $P \subset S$ is *associated* to M if there is an element $m \in M$ with the property that

$$P = \mathrm{Ann}_M(m) = \{f \in S \mid f \cdot m = 0 \in M\}. \tag{2}$$

The module M is *Noetherian* if each submodule is finitely generated (the ring S is Noetherian if it is a Noetherian S–module), and this holds for Noetherian rings if and only if M has a finite presentation (1). The set $\mathrm{Ass}(M)$ of associated primes of a Noetherian module is finite (see Theorem 6.5 in [7]). A Noetherian module is *free* if it has a presentation (1) in which the matrix A comprises zeros, and is *cyclic* if it has a presentation (1) with $k = 1$. A *finite free resolution* of a Noetherian module M is an exact sequence of S–modules and S–module homomorphisms

$$0 \longrightarrow F_n \xrightarrow{\phi_n} \dots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \longrightarrow M \longrightarrow 0 \tag{3}$$

in which each F_i is a free S–module.

A subset U in S is *multiplicative* if it is closed under multiplication. Each multiplicative subset $U \subset S$ defines a *localization*

$$S^U = \{\tfrac{s}{u} \mid s \in S, u \in U\}, \tag{4}$$

where two fractions $\frac{s}{u}$ and $\frac{s'}{u'}$ are identified if there is an element $u'' \in U$ with $u''(u's - us') = 0$. The notation is altered for one special case: if P is a prime ideal in S, then write $S^{(P)}$ for $S^{S \setminus P}$, called the localization at the prime P. For a module M, the same definition as (4) works and defines a localized module M^S or M^P. If the ideal $P = \langle \pi \rangle$ is principal, write $M^{(\pi)} = M^P$. The *dimension* $\dim(S)$ of S is the supremum of the length of chains of distinct prime ideals in S, and this coincides with the supremum of $\dim(S^P)$ over all prime ideals P. The dimension of a localization S^P is also known as the codimension of P, and coincides with the supremum of lengths of chains of prime ideals descending from P.

A ring is *Noetherian* if every ascending chain of ideals stabilizes, is a *local ring* if it has just one maximal ideal, and is *regular* if it is Noetherian and the localization at every prime ideal is a regular local ring. A local ring is a regular local ring if the maximal ideal is generated by exactly d elements where d is the dimension of the local ring. It is clear that R is a regular ring, and it follows (see Chapter 19 of [3]) that any Noetherian R–module has a finite free resolution (3). Notice that the presentation (1) is itself the start of a finite free resolution of M_A:

$$\cdots \longrightarrow R^n \xrightarrow{A} R^k \longrightarrow M_A \longrightarrow 0.$$

If M is a Noetherian R–module with associated primes $\mathrm{Ass}(M) = \{P_1, \dots, P_r\}$, then there is a *prime filtration* of M,

$$M = M_\ell \supset M_{\ell-1} \supset \cdots \supset M_1 \supset M_0 = \{0\}, \tag{5}$$

in which each quotient $M_j/M_{j-1} \cong R/Q_j$ for some prime $Q_j \supset P_i$ for some i (see for example Corollary 2.2 in [10]). The number of times a given prime P_i appears (that is, the number of j for which $Q_j = P_i$) is the *multiplicity* of P_i in the filtration (5). If the prime ideal in question is principal and the module M has no free submodules, then the multiplicity with which P_i appears is independent of the filtration, and we will therefore speak of the multiplicity of P_i in M (see Proposition 6.10 in [6]).

3. Dynamical properties

Let M be any countable R–module, with associated $\mathbb{Z}^d$–action α^M on $X_M = \widehat{M}$. The following result shows how the dynamical properties of α^M may be deduced from the associated primes $\mathrm{Ass}(M)$ of M. All these results are in [11]; we state them here for completeness. A *generalized cyclotomic* polynomial is an element

of R of the form $u_1^{n_1}\dots u_d^{n_d}c(u_1^{m_1}\dots u_d^{m_d})$ for some cyclotomic polynomial c and $\mathbf{n},\mathbf{m}\in\mathbb{Z}^d$. Write $V(P)$ for the set of common zeros of the elements of P in $\mathbb{C}^d$.

Theorem 3.1. *The dynamical system α^M on X_M:*
(a) *satisfies the Descending Chain Condition on closed α^M–invariant subgroups if and only if M is Noetherian;*
(b) *is ergodic if and only if $\{(u_1^{n_1}\dots u_d^{n_d})^k-1\mid \mathbf{n}\in\mathbb{Z}^d\}\not\subset P$ for every $k\geq 1$ and every $P\in\mathrm{Ass}(M)$;*
(c) *is mixing if and only if $u_1^{n_1}\dots u_d^{n_d}-1\notin P$ for each $\mathbf{n}\in\mathbb{Z}^d\backslash\{0\}$ and every $P\in\mathrm{Ass}(M)$;*
(d) *is mixing of all orders if and only if either $P=pR$ for a rational prime p, or $P\cap\mathbb{Z}=\{0\}$ and $\alpha^{R/P}$ is mixing for every $P\in\mathrm{Ass}(M)$;*
(e) *has positive entropy if and only if there is a $P\in\mathrm{Ass}(M)$ that is principal and not generated by a generalized cyclotomic polynomial;*
(f) *has completely positive entropy if and only if $\alpha^{R/P}$ has positive entropy for every $P\in\mathrm{Ass}(M)$;*
(g) *is isomorphic to a Bernoulli shift if and only if it has completely positive entropy;*
(h) *is expansive if and only if M is Noetherian and $V(P)\cap\left(\mathbb{S}^1\right)^d=\emptyset$ for every $P\in\mathrm{Ass}(M)$;*
(i) *has a unique maximal measure if and only if it has finite completely positive entropy.*

Proof. For (a) see Theorem 11.4 in [4]; (b) and (c) are in Theorem 11.2 in [4]; (d) follows from Theorem 3.1 in [12] and Theorem 3.3 in [9]; (e), (f) and (i) are in [6]; (h) is Theorem 3.9 in [10]; (g) is Theorem 1.1 in [8]. □

4. Principal associated primes and entropy

In this section we use localization to find the entropy of α_A^M.

Definition 4.1. Let A be a $k\times n$ matrix of rank k over R. The determinental ideal of A, $J_A\subset R$, is the ideal

$$J_A=\langle f_1,\dots,f_{\binom{n}{k}}\rangle$$

generated by all the $k\times k$ subdeterminants $\{f_1,\dots,f_{\binom{n}{k}}\}$ of A.

For a polynomial $f\in R$, the *logarithmic Mahler measure* of f is defined to be

$$m(f)=\int_0^1\cdots\int_0^1\log|f(e^{2\pi is_1},\dots,e^{2\pi is_d})|\mathrm{d}s_1\dots\mathrm{d}s_d. \tag{6}$$

For brevity, define $m(0)$ to be ∞. Recall from [6] that the entropy of the dynamical system given by the cyclic module R/P, where P is a prime ideal, is given by

$$h\left(\alpha^{R/P}\right)=\begin{cases}0, & \text{if } P \text{ is non–principal;}\\ m(f), & \text{if } P=\langle f\rangle, f\neq 0.\end{cases} \tag{7}$$

More generally, since R is a UFD, for any ideal $Q\subset R$ there is a well–defined greatest common divisor, and

$$h(\alpha^{R/Q})=h(\alpha^{R/\gcd(Q)}),$$

which is zero if $\gcd(Q)=\langle 1\rangle$ and equal to $m(f)$ if $\gcd(Q)=\langle f\rangle$ (see Lemma 4.5 in [2]).

For Noetherian modules,

$$h(\alpha^M) = \sum_{j=1}^{\ell} h(\alpha^{R/Q_j}) \tag{8}$$

where the prime ideals Q_j are the primes appearing in the filtration (5).

Theorem 4.1. *The entropy of α^M is given by*

$$h\left(\alpha^{M_A}\right) = m\left(\gcd(J_A)\right). \tag{9}$$

Before proving this, we indicate some examples.

Example 4.1. (a) Taking $k = n = 1$ and $A = [f]$ with an irreducible polynomial f, we recover the formula (7) in the cyclic case with a principal prime ideal.

(b) Taking $k = 1$ and $n \geq 1$ we recover the general cyclic case.

(c) If $k = n$ then formula (9) simply reduces to $\det(A)$, which was shown in Section 5 of [6].

(d) Let k be an algebraic number field with ring of integers $\mathcal{O}_k$, and f a Laurent polynomial in d variables with coefficients in $\mathcal{O}_k$. The $\mathbb{Z}^d$–dynamical system β dual to multiplication by $u_1, \dots, u_d$ on the $\mathcal{O}_k[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$–module $\mathcal{M} = \mathcal{O}_k[u_1^{\pm 1}, \dots, u_d^{\pm 1}]/\langle f \rangle$ is studied in [2]. Taking an integral basis for $\mathcal{O}_k$ shows that $\mathcal{M}$ as an R–module is of the form (1) with $n = k$, and by (c) we see that

$$h(\beta) = m(\det(A)) = m\left(N_{k:\mathbb{Q}} f\right),$$

recovering Theorem 3.10 in [2].

Lemma 4.1. *Each associated prime of M_A contains J_A.*

Proof. Let B be a $k \times k$ subdeterminant of A. Then for any $\mathbf{v} \in R^k$, $\det(B) \cdot \mathbf{v} = BB^{\mathrm{adj}}\mathbf{v}$. Therefore the annihilator of any element of $M_A \cong R^k/AR^n$ contains $\det(B)$ and also J_A. $\square$

Lemma 4.2. *The principal associated primes of M_A are generated by the irreducible factors of* $\gcd(J_A)$*. Moreover, the multiplicity of each principal associated prime in M is equal to its multiplicity in* $\gcd(J_A)$*.*

Proof. It follows from Lemma 4.1 that each element of the set of principal associated primes of M contains the $k \times k$ subdeterminants of A. This means that the generator of a principal associated prime divides all the subdeterminants and is therefore a factor of $\gcd(J_A)$.

Conversely, let $\{B_i\}$ be the set of $k \times k$ subdeterminants of A, and let

$$\gcd\left(B_1, \dots, B_{\binom{n}{k}}\right) = \pi_1^{e_1} \dots \pi_r^{e_r} \tag{10}$$

be a factorization into irreducibles in R. By Section 2 (5) there is a prime filtration

$$M = M_\ell \supset M_{\ell-1} \supset \cdots \supset M_1 \supset M_0 = \{0\}, \tag{11}$$

with $M_j/M_{j-1} \cong R/Q_j$ with $Q_j \supset P$ for some $P \in \mathrm{Ass}(M)$. Localize (11) at the prime ideal $\langle \pi_1 \rangle$: the pair $M_{j-1} \supset M_j$ localizes to the pair $M_{j-1}^{(\pi_1)} \supset M_j^{(\pi_1)}$, with quotient

$$R^{(\pi_1)}/Q_j^{(\pi_1)} = \begin{cases} R/\langle \pi_1 \rangle & \text{if } Q_j = \langle \pi_1 \rangle; \\ 0. & \text{if not.} \end{cases}$$

So (11) collapses to a shortened filtration of R^{π_1}–modules and we see that the multiplicity of $\langle\pi_i\rangle$ in M coincides with the multiplicity of $\langle\pi_i\rangle$ in $M^{(\pi_i)}$ for each $i = 1, \dots, r$.

We are therefore reduced to studying the local case: let π be any one of the π_i's, and write

$$M_A^{(\pi)} = \left(R^{(\pi)}\right)^k / A\left(R^{(\pi)}\right)^n.$$

We can change our matrix by invertible (over $R^{(\pi)}$) elementary row operations and this gives us an isomorphic module with the same subdeterminants. In $R^{(\pi)}$ define $\mathrm{ord}(f) = \mathrm{ord}_\pi(f)$ to be the number of times that π divides into f. Write $f \le g$ if $\mathrm{ord}(f) \le \mathrm{ord}(g)$, and with respect to this partial ordering find (one of) the smallest entries in A. Permute rows and columns in A so that a_{11} is a smallest entry. Then $a_{i1} \ge a_{11}$ for $2 \le i \le k$ so the quotient a_{i1}/a_{11} is an element of $R^{(\pi)}$ and we can subtract multiples of the first row from the others to get a matrix of the form

$$A_1 = \begin{bmatrix} a_{11} & \dots & \\ 0 & & \\ \vdots & & * \\ 0 & & \end{bmatrix}$$

Repeat with a_{22} and so on to produce a matrix of the form

$$A_* = \begin{bmatrix} a_{11} & \dots & & & \\ 0 & a_{22} & \dots & & \\ \vdots & 0 & & & \\ 0 & \dots & 0 & a_{kk} & \dots \end{bmatrix}$$

in which each a_{jj} is in turn the smallest non–zero element of the submatrix $(a_{st})_{s,t\ge j}$. Let $\mathrm{ord}(a_{jj}) = e_{jj}$ for each j.

Now let $\mathbf{v} = (1, 0, \dots, 0)^t$, so that

$$\mathrm{Ann}(\mathbf{v} + A_* R^n) = \langle a_{11}\rangle,$$

since the other columns of the matrix have a first component which is divisible by a_{11}. The map $f \mapsto f \cdot \mathbf{v} \in M^{(\pi)}$ gives a filtration

$$\mathbf{v}R^{(\pi)} \supset \pi\mathbf{v}R^{(\pi)} \supset \dots \supset \pi^{(e_{11}-2)}\mathbf{v}R^{(\pi)} \supset \pi^{(e_{11}-1)}\mathbf{v}R^{(\pi)} \supset 0$$

of submodules of $M_A^{(\pi)}$. As the same argument works for the other standard basis vectors it follows that the multiplicity of π in $M_A^{(\pi)}$ is $\sum e_{jj}$. Calculating all the subdeterminants shows that the greatest common divisor is equal to the product $\prod_j a_{jj} = \pi^{\sum_j e_{jj}}$. So the multiplicity of π in $\gcd(J_A)$ is equal to the multiplicity of the associated prime (π) in a prime filtration of M_A. □

Proof of Theorem 4.1. Use Lemma 4.2 and Section 2 to find the principal associated primes and their multiplicites; the result follows by (8). □

For an ideal P in R, recall that $V(P) = \{\mathbf{z} \in \mathbb{C}^d \mid f(\mathbf{z}) = 0 \ \forall\ f \in P\}$ denotes the set of common zeros of P. Write $V(f)$ for $V(\langle f\rangle)$. By Theorem 3.1, α^M is expansive if and only if $V(P) \cap (\mathbb{S}^1)^d = \emptyset$ for each associated prime $P \in \mathrm{Ass}(M)$.

Theorem 4.2. *Let M_A be a finitely presented module with A of rank k. Then α^{M_A} is expansive if and only if*

$$(\mathbb{S}^1)^d \cap \left(\bigcap_{j=1,\dots,\binom{n}{k}} V(\det(B_j)) \right) = \emptyset, \tag{12}$$

where $\{B_j\}$ is the set of $k \times k$ subdeterminants of A.

Proof. Assume first that

$$\mathbf{z} \in (\mathbb{S}^1)^d \cap \left(\bigcap_{j=1,\dots,\binom{n}{k}} V(\det(B_j)) \right).$$

Assume that for every associated prime P of M_A there is a polynomial $f_P \in P$ for which $f_P(\mathbf{z}) \neq 0$. Then let $f = \prod_{P \in \mathrm{Ass}(M)} f_P$ (so $f(\mathbf{z}) \neq 0$). From a prime filtration of M_A it is clear that for some power m,

$$f^m M = 0. \tag{13}$$

On the other hand, since $\mathbf{z}$ was chosen to lie in the set of common zeros of all the subdeterminants, in the ring

$$M(\mathbf{z}) = \frac{\mathbb{Z}[\mathbf{z}^{\pm 1}]^k}{A(\mathbf{z})\mathbb{Z}[\mathbf{z}^{\pm 1}]^n}$$

we have that all $k \times k$ subdeterminants of $A(\mathbf{z})$ vanish, so $\mathrm{rank}(A(\mathbf{z})) < k$, and in particular $M(\mathbf{z}) \neq 0$, contradicting (13). It follows that if the intersection in (12) contains a point $\mathbf{z}$ then this point must lie in $V(P)$ for some associated prime P, showing that α^{M_A} is not expansive by Theorem 3.1.

Conversely, if α^{M_A} is not expansive, then there is an associated prime $P \in \mathrm{Ass}(M_A)$ with $V(P) \cap (\mathbb{S}^1)^d \ni \mathbf{z}$ say. However the associated prime P must contain all the subdeterminants by Lemma 4.1. so $\mathbf{z} \in \bigcap_{j=1,\dots,\binom{n}{k}} V(\det(B_j))$. □

5. The square case

As remarked in Theorem 3.1, various dynamical properties of systems of the form α^M are governed by properties of the set $\mathrm{Ass}(M)$ of associated primes of M. In this section we show that the associated primes of a finite presentation with $k = n$ (the "square case") are all visible in the determinant of the matrix of relations, so the dynamics are as easy to deduce as in the case of a cyclic module with a single principal associated prime. We also calculate the periodic points because *a priori* one needs more information than the associated primes to calculate this (see Section 7 of [6]).

Lemma 5.1. *If the finitely–presented module M_A has $k = n$ and A has maximal rank, then the associated prime ideals of M are all given by irreducible factors of* $\det(A)$.

Proof. Let $\det(A) = \pi_1^{e_1} \dots \pi_r^{e_r}$ be the decomposition into irreducibles. By linear algebra over the quotient field of R we know that $w \in AR^n$ if and only if $\frac{1}{\det A} A^{\mathrm{adj}} w \in R^n$. If an element $\mathbf{v} + AR^n$ has $\mathrm{Ann}(\mathbf{v} + AR^n) = P$ for some $P \in \mathrm{Ass}(M_A)$, then

$$P = \{ f \in R \mid \frac{f}{\det(A)} A^{\mathrm{adj}} \mathbf{v} \in R^k \}.$$

Now in $\frac{1}{\det(A)}A^{\mathrm{adj}}v$ after all possible cancellations there must be some π_i in the denominator (since $\mathbf{v} \notin AR^k$). Let this denominator be g say; then g must divide f for all $f \in P$, so $\mathrm{Ann}(\mathbf{v} + AR^n) = \langle g \rangle$. As P is prime the element g must be irreducible. It follows that all the associated primes of M_A are principal and arise as factors of the determinant of A.

It is easy to see that the argument above also proves that each irreducible factor of $\det A$ gives an associated prime (or use Lemma 4.2) for the reverse inclusion. □

Corollary 5.1. *The dynamical system α^{M_A} for a square matrix A is ergodic, mixing, mixing on a shape F, mixing of all orders, K, if and only if the corresponding cyclic system $\alpha^{R/\langle\det(A)\rangle}$ has the same property.*

We are also able to compute directly the periodic points in such systems. A *period* for a $\mathbb{Z}^d$–action α on X is a lattice $\Lambda \subset \mathbb{Z}^d$ of full rank; the size of the period is the (finite) index $|\mathbb{Z}^d/\Lambda|$. The set of points of period Λ is

$$\mathrm{Fix}_\Lambda(\alpha) = \{x \in X \mid \alpha_{\mathbf{n}}x = x \ \forall \ \mathbf{n} \in \Lambda\}.$$

Since the (multiplicative) dual group of $\mathbb{Z}^d$ is $(\mathbb{S}^1)^d$, the annihilator $\Lambda^\perp$ of Λ is a subgroup of $(\mathbb{S}^1)^d$ with cardinality $|\mathbb{Z}^d/\Lambda|$.

Lemma 5.2. *If A is a square matrix of maximal rank, then*

$$\mathrm{Fix}_\Lambda\left(\alpha^{M_A}\right) = \begin{cases} \infty & \text{if } \prod_{\mathbf{z}\in\Lambda^\perp} |\det(A)(\mathbf{z})| = 0; \\ \prod_{\mathbf{z}\in\Lambda^\perp} |\det(A)(\mathbf{z})| & \text{if not.} \end{cases}$$

Proof. For brevity we prove this for square periods $\Lambda_n = n\mathbb{Z}^d$; the general case is similar but notationally unpleasant. We follow the method used in [6], Section 7, exactly.

An element $\mathbf{x} \in X = \widehat{R^k/AR^k}$ is periodic with respect to Λ_n if it annihilates $J(\Lambda_n)R^k$ where $J(\Lambda_n) = \langle u_1^n - 1, \dots, u_d^n - 1\rangle$. So the periodic points are exactly the elements in the dual group of

$$R^k/(AR^k + J(\Lambda_n)^k). \tag{14}$$

Therefore the number of periodic points is equal to the number of elements in (14) whenever this quantity is finite or is infinite if not. As $R/J(\Lambda_n)$ is isomorphic to $\mathbb{Z}^{n^d}$ we see that the module (14) is isomorphic to $(\mathbb{Z}^F)^k/B(\mathbb{Z}^F)^k$ where $F = \{1, \dots, n\}^d$ and B is obtained from A by interpreting the variable u_ℓ as the shift of the ℓ-th coordinate in F. The number of periodic points in X is now given by the determinant of B (or is infinite if $\det B = 0$). We calculate this quantity using a suitable basis of $(\mathbb{C}^F)^k$. The elements in this vector space have the form $(w_{\binom{\mathbf{e}}{\mathbf{i}}})_{\binom{\mathbf{e}\in F}{i\in[1,k]}}$; use the basis

$$v_{\mathbf{f}}^j = (\delta_{ij}\omega^{f_1e_1+\cdots+f_de_d})_{\binom{\mathbf{e}}{\mathbf{i}}}.$$

where ω is a primitive n-th root. In this basis the matrix B becomes

$$C = (a_{ij}(\omega^{e_1}, \dots, \omega^{e_d})\delta_{\mathbf{ef}})_{\binom{\mathbf{e}}{\mathbf{i}}\binom{\mathbf{f}}{\mathbf{j}}}$$

because the shift of the ℓ-th coordinates in F has $v_{\mathbf{f}}^j$ as eigenvector with eigenvalue ω^{f_ℓ}. The determinants are given by

$$\det(B) = \det(C) = \prod_{\mathbf{e}\in F} \det(A)(\omega^{e_1}, \dots, \omega^{e_d}),$$

Because the matrix C can be viewed as being of the form

$$\begin{bmatrix} D_1 & 0 & 0 & \dots & 0 \\ 0 & D_2 & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & & \dots & 0 & D_{|F|} \end{bmatrix}$$

where the submatrices D_j are obtained from A by evaluation at $(\omega^{e_1}, \dots, \omega^{e_d})$ for some $(e_1, \dots, e_d) \in F$. The determinant of such a matrix is the product of the determinants of the submatrizes. $\square$

For a lattice Λ, let $g(\Lambda) = \min_{\mathbf{n} \in \Lambda \setminus \{0\}} \{\|\mathbf{n} - \mathbf{0}\|\}$. The characterization of expansiveness and Lemma 5.2 gives a very simple proof of the general result that the growth rate of periodic points coincides with the entropy for expansive algebraic $\mathbb{Z}^d$–actions (see Section 7 of [6]) for finitely presented systems with $k = n$.

Corollary 5.2. *If A is a square matrix of maximal rank, and $V(\det(A)) \cap (\mathbb{S}^1)^d = \emptyset$, then the growth rate of periodic points is equal to the entropy:*

$$\lim_{g(\Lambda) \to \infty} \frac{1}{|\mathbb{Z}^d/\Lambda|} \log \operatorname{Fix}(\alpha^{M_A}) = h(\alpha^{M_A}).$$

6. The general case

In this section we simply describe the appropriate results from commutative algebra and indicate by examples how they may be used to compute associated primes in the general case.

Fix the finite presentation (1) of a Noetherian R–module M. For each R–module map $\phi : R^a \to R^b$ define $J(\phi)$ to be the ideal generated by the $\operatorname{rank}(\phi) \times \operatorname{rank}(\phi)$ subdeterminants of a matrix for ϕ. For maps ϕ appearing in a finite free resolution, these ideals are the *Fitting ideals* of the module. By convention 0×0 determinants give the trivial ideal $\langle 1 \rangle$.

Theorem 6.1. *Let*

$$0 \longrightarrow F_n \xrightarrow{\phi_n} \dots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \longrightarrow M_A \longrightarrow 0 \tag{15}$$

be a finite free resolution of the R–module M_A. Let P be a prime ideal of R with $\dim(R^P) = \ell$. Then $P \in \operatorname{Ass}(M_A)$ if and only if $P \supset J(\phi_\ell)$.

Proof. This is proved in Corollary 20.14 of [3] with the condition $\dim(R^P) = \ell$ replaced by $\operatorname{depth}(P \subset R) = \ell$ (see Chapter 18 of [3] for this notion). By Theorem 18.7 of [3] we have that since R is regular (and hence Cohen–Macaulay by Section 18.5 of [3]), $\operatorname{depth}(P) = \operatorname{height}(P) := \dim(R^P)$, so the result follows. $\square$

Notice that the first Fitting ideal $J(\phi_1)$ is exactly the ideal J_A used above.

We now describe several examples to illustrate the kind of calculations involved and some of the phenomena that may arise.

Example 6.1. (a) Let $P = \langle f \rangle$ be a prime ideal. Then a finite free resolution of R/P is given by

$$0 \longrightarrow R \xrightarrow{[f]} R \longrightarrow R/P \longrightarrow 0.$$

By Theorem 6.1, we see that the associated primes of R/P comprise exactly $\{P\}$.

(b) Let f be irreducible, and let $M = R/\langle 2f\rangle$. Then

$$0 \longrightarrow R \xrightarrow{[2f]} R \longrightarrow M \longrightarrow 0.$$

is a free resolution of M. If $\dim(P) = 1$ then $P \in \mathrm{Ass}(M)$ if and only if $P \supset J([2f]) = \langle 2f\rangle$, so $P = \langle 2\rangle$ or $\langle f\rangle$. Notice that $J(\phi_2) = \langle 1\rangle$ so there are no further primes, so $\mathrm{Ass}(M) = \{\langle 2\rangle, \langle f\rangle\}$.

(c) The simplest setting in which a higher Fitting ideal appears is Ledrappier's example. Let $M = R/\langle 2, 1+u_1+u_2\rangle$. A simple syzygy calculation gives the free resolution

$$0 \longrightarrow R \xrightarrow{\phi_2} R^2 \xrightarrow{\phi_1} R \longrightarrow M \longrightarrow 0,$$

where $\phi_1 = \begin{bmatrix}1+u_1+u_2, 2\end{bmatrix}$ and $\phi_2 = \begin{bmatrix}1+u_1+u_2\\ -2\end{bmatrix}$. If $\dim(P) = 1$ then $P \in \mathrm{Ass}(M)$ if and only if $P \supset J([1+u_1+u_2, 2]) = \langle 2, 1+u_1+u_2\rangle$, so there are no primes here. If $\dim(P) = 2$ then $P \in \mathrm{Ass}(M)$ if and only if $P \supset J(\begin{bmatrix}1+u_1+u_2\\ -2\end{bmatrix}) = \langle 2, 1+u_1+u_2\rangle$, giving the one associated prime $\langle 2, 1+u_1+u_2\rangle$.

(d) Let $A = \begin{bmatrix}2 & u_2^2-5 & 0\\ 0 & u_1u_2-7u_1+u_2 & 3\end{bmatrix}$. Then the first Fitting ideal $J(A)$ is generated by the set $\{2u_1u_2 - 14u_1 + 2u_2, 6, 3u_2^2 - 15\}$. A principal prime ideal which contains $J(A)$ must contain 6, and must therefore be generated by 2 or 3: in either case it cannot contain the other two generators of $J(A)$. This proves that no principal ideals are associated to the module R^2/AR^3. Using the special form of the matrix we see that the kernel of A in R^3 is generated by the vector

$$v = \begin{bmatrix}3u_2^2 - 15\\ -6\\ 2u_1u_2 - 14u_1 + 2u_2\end{bmatrix}.$$

The second Fitting ideal $J(v)$ is equal to the first. Assume P is prime with $\dim(R^P) = 2$ and $P \supset J(v)$. Then this prime contains either 2 or 3. If $3 \in P$ then P lies above the prime $\langle 3, u_1u_2 - 7u_1 + 2u_2\rangle$ which is the only one with $\dim(R^P) = 2$. For the case $2 \in P$ we have also $u_2^2 - 5 \in P$ but this element is modulo 2 congruent to $(u_2-1)^2$; this means that the only prime with the correct local dimension containing 2 is $P = \langle 2, u_2 - 1\rangle$. The only associated primes of $M = R^2/AR^3$ are therefore $P_1 = \langle 3, u_1u_2 - 7u_1 + 2u_2\rangle$ and $P_2 = \langle 2, u_2 - 1\rangle$. The corresponding dynamical system is expansive and ergodic but not mixing, and has zero entropy.

(e) Let $A = \begin{bmatrix}2 & 3u_2+5 & 3u_1-3u_2\\ u_1-4 & u_1-1 & 3u_1-6\end{bmatrix}$. Then the first Fitting ideal is generated by

$$-3u_1 + 18 - 3u_1u_2 + 12u_2,$$
$$18u_1 - 12 - 3u_1^2 + 3u_1u_2 - 12u_2 \text{ and}$$
$$-21u_2 - 30 - 3u_1^2 + 18u_1 + 12u_1u_2.$$

The only principal ideal above $J(A)$ is $\langle 3\rangle$. With a computer algebra system one can calculate the kernel of the map A: it is generated by the vector

$$v = \begin{bmatrix} -7u_2 - 10 - u_1^2 + 6u_1 + 4u_1u_2 \\ 4 + u_1^2 - 6u_1 - u_1u_2 + 4u_2 \\ 6 - u_1u_2 + 4u_2 - u_1 \end{bmatrix}.$$

The second Fitting ideal $J(v)$ is generated by the components of this vector and one can calculate that

$$\{u_1 - 3u_2 - 4, 3u_2^2 + 3u_2 - 2\}$$

is also a generating set. So $J(v)$ is a prime with local dimension 2. The only associated primes of the module R^2/AR^3 are $\langle 3\rangle$ and $\langle u_1 - 3u_2 - 4, 3u_2^2 + 3u_2 - 2\rangle$. The entropy of the corresponding dynamical system is $\log 3$, but the system does not have completely positive entropy. The ring $R/J(v)$ is isomorphic to a subring of $\mathbb{Q}[\sqrt{\frac{11}{12}}]$ via the map sending u_2 to $-\frac{1}{2} + \sqrt{\frac{11}{12}}$ (a root of $3y^2 + y - 2 = 0$), and u_1 to $\frac{5}{2} + \sqrt{\frac{33}{4}}$. The field-theoretic norms of those two elements are -2 and $-\frac{2}{3}$ respectively. It follows that there can be no nontrivial $(n_1, n_2) \in \mathbb{Z}^2$ such that $u_1^{n_1}u_2^{n_2} - 1 \in J(v)$ because this would yield $2^{n_1}(\frac{2}{3})^{n_2} = 1$. The dynamical system is therefore mixing of all orders and ergodic.

(f) Even in the square ($n = k$) case the first Fitting ideal does not contain enough information to construct a prime filtration of the module. The following type of example is well–known (see for example Remark 6(5) in [13] or Example 5.3(2) in [11]). Let $A = \begin{bmatrix} 4 - u_1 & 1 \\ 1 & -u_1 \end{bmatrix}$ and $B = \begin{bmatrix} 3 - u_1 & 2 \\ 2 & 1 - u_1 \end{bmatrix}$. Then $\det(A) = \det(B)$ so the systems α^{M_A} and α^{M_B} have the same entropy, number of periodic points, and in fact are both isomorphic to Bernoulli shifts and hence measurably isomorphic. Both modules M_A and M_B have similar finite free resolutions,

$$0 \longrightarrow R^2 \xrightarrow{\phi} R^2 \longrightarrow M \longrightarrow 0,$$

where $\phi = A$ for $M = M_A$ and $\phi = B$ for $M = M_B$. It is easy to check that $M_A \cong R/\langle u_1^2 - 4u_1 - 1\rangle$, so that

$$M_A \supset 0$$

is a prime filtration. On the other hand, the shortest filtration of M_B is of the form

$$M_B \supset N \supset 0,$$

with first quotient $N/\{0\} \cong R/\langle u_1^2 - 4u_1 - 1\rangle$, and second quotient

$$M/N \cong R/\langle u_1^2 - 4u_1 - 1\rangle + Q$$

for some ideal $Q \not\subset \langle u_1^2 - 4u_1 - 1\rangle$.

(g) Let f, g, h be co–prime elements of R, and consider the module $M = R/[f, g, h]R^3$. Then a finite free resolution is given by the Koszul complex

$$0 \longrightarrow R \xrightarrow{\phi_1} R^3 \xrightarrow{\phi_2} R^3 \xrightarrow{\phi_3} R \longrightarrow M \longrightarrow 0,$$

in which $\phi_1 = \begin{bmatrix} f \\ g \\ h \end{bmatrix}$, $\phi_2 = \begin{bmatrix} 0 & h & -g \\ -h & 0 & f \\ g & -f & 0 \end{bmatrix}$ and $\phi_3 = [f, g, h]$.

(h) An example in which the rank of the presenting matrix is too small is given by $A = \begin{bmatrix} 2 \\ 1+u_1+u_2 \end{bmatrix}$. Let $M = M_A$; then $\mathrm{Ann}_M \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \langle 0 \rangle$, so M has a free submodule $L = \begin{pmatrix} 1 \\ 0 \end{pmatrix} R$. The corresponding dynamical system therefore has as a factor the full shift with circle alphabet, so $h(\alpha^M) = \infty$. The quotient $M/L \cong R/\langle 1+u_1+u_2 \rangle$ is then of the form (1). Of course the free submodule sits inside M in many different ways, so there is no "canonical" quotient M/L.

(i) The simplest examples of algebraic dynamical systems without finite presentation are certain non–expansive automorphisms of solenoids, as studied in [5] and [1]. Let $X = \widehat{\mathbb{Z}[\frac{1}{6}]}$, and let α be the automorphism of X dual to $x \mapsto 2x$ on $\mathbb{Z}[\frac{1}{6}]$ (here $d = 1$). The R–module corresponding to the dynamical system then has a chain of submodules

$$\mathbb{Z}[\tfrac{1}{2}] \subset \tfrac{1}{3}\mathbb{Z}[\tfrac{1}{2}] \subset \tfrac{1}{9}\mathbb{Z}[\tfrac{1}{2}] \subset \dots,$$

each of which is isomorphic as an R–module to $R/\langle u_1 - 2 \rangle$, that never stabilizes. It follows that the corresponding module is not Noetherian.

References

[1] V. Chothi, G. Everest and T. Ward. S-integer dynamical systems: periodic points. *Journal für die Riene und. Angew.*, 489:99-132, 1997.

[2] M. Einsiedler. A generalisation of Mahler measure and its application in algebraic dynamical systems. *Acta Arithmetica, to appear.*

[3] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry.* Springer Verlag, New York, 1995.

[4] B. Kitchens and K. Schmidt. Automorphisms of compact groups. *Ergodic Theory and Dynamical Systems*, 9:691–735, 1989.

[5] D.A Lind and T. Ward. Automorphisms of solenoids and p-adic entropy. *Ergodic Theory and Dynamical Systems*, 8:411–419, 1988.

[6] D.A. Lind, K. Schmidt, and T. Ward. Mahler measure and entropy for commuting automorphisms of compact groups. *Inventiones Math.*, 101:593–629, 1990.

[7] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, Cambridge, 1986.

[8] D.J. Rudolph and K. Schmidt. Almost block independence and Bernoullicity of Z^d actions by automorphisms of compact abelian groups. *Inventiones Math.*, 120:455–488, 1995.

[9] K. Schmidt. Mixing automorphisms of compact groups and a theorem by Kurt Mahler. *Pacific Journal of Math.*, 137:371-385, 1989.

[10] K. Schmidt. Automorphisms of compact abelian groups and affine varieties. *Proceedings of the London Math. Soc.*, 61:480–496, 1990.

[11] K. Schmidt. *Dynamical Systems of Algebraic Origin.* Birkhäuser, Basel, 1995.

[12] K. Schmidt and T. Ward. Mixing automorphisms of compact groups and a theorem of Schlickewei. *Inventiones Math.*, 111:69–76, 1993.

[13] T. Ward. The Bernoulli property for expansive Z^2 actions on compact groups. *Israel Journal of Math.*, 79:225–249, 1992.

Mathematisches Institut, Universität Wien, Strudlhofgasse 4, A-1090 Vienna, Austria
E-mail address: manfred@nelly.mat.univie.ac.at

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.
E-mail address: t.ward@uea.ac.uk